REMARKS

These remarks are set forth in response to the Second Office Action. As this amendment has been timely filed within the three-month statutory period, neither an extension of time nor a fee is required. At the time of the Second Office Action, Claims 1 through 21 were pending and rejected in this application. Applicants have cancelled claims 8 through 21 to remove these claims from further consideration in this application. Applicants are not conceding in this application that those claims are not patentable over the prior art cited by the Examiner, as the present claim cancellations are only for facilitating expeditious prosecution of the present application. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

CLAIMS 1-3, 8-10 AND 15-17 ARE REJECTED UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON FRID, U.S. APPLICATION PUBLICATION NO. 2004/0030877 (HEREINAFTER FRID) IN VIEW OF GRIFFIN ET AL., U.S. APPLICATION PUBLICATION NO. 2002/0194482 (HEREINAFTER FRID) AND FURTHER IN VIEW OF KIM ET AL., U.S. PATENT NO. 6,487,656 (HEREINAFTER KIM)

On pages 2-3 of the Second Office Action, the Examiner asserted that one having ordinary skill in the art would have been realistically impelled to modify Frid in view of Griffin and in further view of Kim to arrive at the claimed invention. This rejection is respectfully traversed.

<u>**Claim 1**</u>

Independent claim 1 recites a method for "**reducing the boot time** of a Trusted Computing Performance Alliance (TCPA) based computing system" includes "executing a **boot block code** comprising a **Core Root of Trust for measurement (CRTM)**". As an initial matter, there is no discussion or mention in Frid of "**reducing the boot time of a Trusted Computing Performance Alliance (TCPA) based computing system**" by "executing a **boot block code** comprising a **Core Root of Trust for measurement (CRTM)**". To the contrary, the Frid invention is specifically directed to a method that "implement[s] <u>**embedded controller firmware updating**</u>." (see lines 6-8 of paragraph [0005] of Frid, emphasis added). Moreover, Frid explicitly states that Figure 2 is a diagram "illustrating an exemplary <u>**embedded controller firmware updating method 30**</u> in accordance with the principles of the present invention." (see lines 1-4, paragraph [0021] of Frid, emphasis added). Thus, paragraph [0022] and Figure 2 does not support the Examiner's conclusion that Frid discloses a method for "<u>**reducing the boot time**</u> of a ... <u>**TCPA based**</u> computing system".

Independent claim 1 further recites "**reading bits in a register** … wherein **said bits in said register indicate <u>whether segments</u> of said flash memory have been updated**". Referring to page 2 of the Second Office Action, the Examiner cited paragraph [0022] and Figure 2, item 33 of Frid to teach " reading bits in register storing boot code, where register indicates whether segments have been updated." Applicants, however, disagree that this passage teaches the limitations for which Frid is being relied upon to teach. Frid teaches "reading firmware identification data from the embedded controller and comparing it with corresponding data in the system BIOS." Notably, Fig. 2, item block 33 is silent as to where the "firmware identification data" resides and what the "firmware identification data" indicates. More importantly, there is no discussion in Frid of "**reading bits in a register** … wherein **said bits in said register indicate <u>whether segments</u> of said flash memory have been updated**". Instead of providing that the firmware of the embedded controller will be stored in multiple segments of flash memory, Frid explicitly teaches **<u>a single wholesale replacement of the embedded controller's firmware</u>**. (see lines 8-11 of paragraph [0026] of Frid; "new firmware image file … **<u>overwriting</u>** the existing firmware."). Thus, Fig. 2, item block 33 of Frid fails to teach the limitations for which the Examiner is relying upon Frid to teach.

To teach the claimed "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of **said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS have not been updated" the Examiner cited paragraphs [0052], [0056], [0061], and Figs. 5 & 7 of Griffin. However, upon reviewing the Examiner's cited passages Applicants are unable to identify where Griffin teaches "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a POST BIOS if one or more of **said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS have not been updated". In direct contrast, Griffin teaches creating "integrity metrics" to be provided in response to an integrity challenge to use a "guest operating system 25" (see lines 9-14 of paragraph [0048] of Griffin. Moreover, claim 1 recites "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a POST BIOS **if one or more of said bits in said register indicate one or more segments** of said flash memory storing said POST

BIOS **have not been updated**," whereas Griffin teaches updating an "integrity metric" **if it has been updated**. Thus Griffin fails to teach the limitations for which the Examiner is relying upon Griffin to teach.

Regarding the Examiner's obviousness analysis, the Examiner asserted the following on page 4 of the First Office Action:

> It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the obtaining values from table storing hashed values form previous measurement of BIOS if segments of flash memory have not been updated in the invention of Frid in order to provide integrity check and periodical update as taught in Par. 0012. Kim further discloses the POST activities see Fig. 6 item 602, and this action can be modified by Griffin who uses has of BIOS to check to see updates so that POST activities (i.e., system activities) as well as BIOS activities (processor activities) is checked see Fig. 3 item 310 & 320

Applicants are unclear as to how the Examiner's proposed rationale for the combination would have led one having ordinary skill in the art to modify Frid in view of Griffin and in further view of Kim. As indicated in the analysis above, Griffin does not teach "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a POST BIOS **if one or more of said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS **have not been updated**," To the contrary, Griffin teaches updating an entire "integrity metric" **if that metric has been updated**.

CLAIMS 4-7, 11-14 AND 18-21 ARE REJECTED UNDER 35 U.S.C. § 103 AS BEING UNPATENTABLE OVER FRID IN VIEW OF GRIFFIN, FURTHER IN VIEW OF KIM AND FURTHER IN VIEW OF POLYUDOV, U.S. APPLICATION PUBLICATION NO. 2004/0186988 (HEREINAFTER POLYUDOV)

Claims 2-7 depend ultimately from independent claim 1, and Applicants incorporate herein the arguments previously advanced in traversing the imposed rejection of claim 1 under 35 U.S.C. § 103 for obviousness based upon Frid, Griffin and Kim. The tertiary reference to Polyudov does not cure the argued deficiencies of the combination of Frid, Griffin and Kim. Accordingly, even if one having ordinary skill in the art were motivated to combine the applied prior art, the proposed combination of references would not yield the claimed invention.

For these reasons, the Applicants respectfully request the withdrawal of the rejections under 35 U.S.C. § 103(a). This entire application is now believed to be in condition for allowance and such action is respectfully requested. The Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: March 13, 2008

/Steven M. Greenberg/

Steven M. Greenberg
Reg. No.: 44,725
Customer Number 50594
Attorney for Applicant(s)
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Fax: (561) 244-1062